

### **REMARKS**

Reconsideration of the application and allowance of the pending claims are respectfully requested based upon the remarks below.

Claims 1-2, 10-12 are rejected under 35 USC 102(b) as being anticipated by Griffin (US 2002/0194496). In addition, claims 3-9 are rejected under 35 USC 103(a) as being unpatentable over Griffin in view of Wiseman (US 2004/0003288). Applicants respectfully traverse these rejections for the reasons discussed below.

#### **Rejections under 35 USC 102**

Independent claim 1 recites, *inter alia*, a system comprising a trusted computer platform that includes at least one first logically protected computing compartment, at least one second logically protected computing compartment, and at least one security rule, wherein:

“the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled.” (Emphasis added).

In other words, claim 1 recites wherein security rules are only loaded when services associated with the rules are enabled. The Office Action (OA) posits that Griffin, at paragraph [0034], discloses this feature. Appellants respectfully disagree.

At the cited paragraph, although Griffin appears to indicate that access to communication interfaces is governed by rules specified on a compartment to compartment basis, and that a dynamically loadable security module consults a table of rules indicating which compartments are allowed to access the resources of another compartment, nowhere does Griffin disclose, teach, or suggest when these rules are loaded.

Applicants respectfully submit that the Examiner has mischaracterized the function of the cited "dynamically loadable security module." Based upon the context of paragraph [0034] Applicants further submit that the disclosed security module appears to only relate to a program that uses already loaded rules to determine whether compartments are allowed access to resources. In other words, Applicants suggest that Griffin appears to indicate that the security module is merely a monitoring program that checks for the presence of previously loaded rules. Nowhere does Griffin indicate when these rules are loaded, let alone suggesting that the rules are loaded only as required by the enabling of resources in a subsequently loaded compartment, as recited in claim 1.

Indeed, Applicants' interpretation is supported by additional language in paragraph [0034] that further describes wherein the program, in the absence of a rule explicitly allowing a cross compartment access, an access attempt is denied. In other words if access is not explicitly allowed, access is denied. No mention is made of loading a rule based upon resources of a newly loaded compartment being enabled.

A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Accordingly, because Griffin does not disclose, teach or suggest at least the above feature recited in claim 1, Applicants recited method is distinguished over Griffin and therefore the rejection of claim 1 under 35 U.S.C. §102(b) is improper.

Applicants respectfully submit, therefore, that independent claim 1, and claims 2, 10, and 11 that depend therefrom, are patentable over Griffin.

Regarding independent claim 12, Applicants submit that claim 12 is similar to claim 1, reciting wherein:

loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled. (Emphasis added)

Based upon the failure of Griffin to disclose this above feature, as presented above relative to claim 1, Applicants respectfully submit that claim 12 is likewise allowable over Griffin.

Withdrawal of the anticipation rejection over Griffin is respectfully requested.

**Rejections under 35 USC 103**

The rejection of claims 3-9 as being obvious over Griffin in view of Wiseman is respectfully traversed.

Applicants respectfully submit that, as discussed above, independent claim 1 is patentable over Griffin for the failure of Griffin to disclose, teach, or suggest "wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled."

Applicants further submit that Wiseman fails to remedy the deficiencies of Griffin as applied to claim 1. Accordingly, claim 1 is patentable over the applied references, and claims 3-9 are likewise patentable over the asserted combination of references at least in view of their dependence on claim 1. Withdrawal of the rejection is respectfully requested.

**Conclusion**

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

Early issuance of a Notice of Allowance is courteously solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

**Michael John WRAY et al.**



Kenneth M. Berner  
Registration No. 37,093

**HEWLETT-PACKARD COMPANY**

Intellectual Property Administration

P. O. Box 272400

Fort Collins, CO 80527-2400

703-684-1111 Telephone

970-898-0640 Telecopier

**Date: November 11, 2008**

**KMB/ERM/cac**